

(43) 公開日 平成16年8月10日(2004.8.10)

テーマコード (参考)
5B089

審査請求 未請求 請求項の数 23 O L (全 26 頁)

(71) 出願人 000003078
株式会社東芝
東京都港区芝浦一丁目1番1号

(74) 代理人 100083161
弁理士 外川 英明

(72) 発明者 菅野 伸一
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72) 発明者 楢岡 正道
東京都府中市東芝町1番地 株式会社東芝
府中事業所内

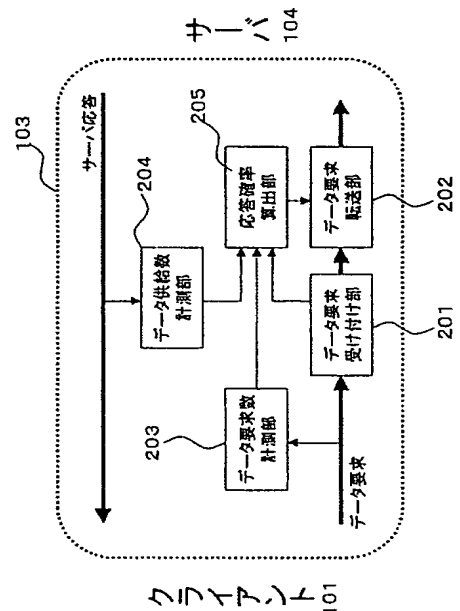
Fターム(参考) 5B089 GA00 KA17 KB11 KB13 KC29
KC52 MA01 MA07

(54) 【発明の名称】 サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機

(57) 【要約】

【課題】不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながら、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置を提供することを目的とする。

【解決手段】サーバとなる計算機に対してデータ要求される数と、これに応答するサーバのデータ応答の数を用いてサーバ計算機の負荷状態を求め、この負荷状態に応じてサーバに転送するデータ要求の割合を変化させる手段を備えたサーバ計算機保護装置とする。



【特許請求の範囲】

【請求項 1】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ供給数計測手段と、前記データ供給数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置。

【請求項 2】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するデータ供給数計測手段と、前記データ要求数計測手段及びデータ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置。

【請求項 3】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、前記サーバ計算機から該サーバ計算機の処理状況に関する情報を受信する処理情報受信手段と

前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置。

【請求項 4】

- 10 不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、前記サーバ計算機から、前記データ要求受け付け手段で受け付けた前記所定のクライアント計算機のデータ要求に対する、該サーバ計算機が実行している処理の状況に関する情報を受信する処理情報受信手段と前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置。

【請求項 5】

- 30 前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 1 または請求項 2 に記載のサーバ計算機保護装置。

【請求項 6】

- 40 前記サーバ計算機の負荷状態を値として記憶する負荷状態記憶手段をさらに備え、前記サーバ負荷算出手段は、求めた前記サーバ計算機の負荷状態に応じて前記負荷状態記憶手段に記憶した値を増減し、前記データ要求転送手段は、前記負荷状態記憶手段に記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 1 または請求項 2 に記載のサーバ計算機保護装置。

【請求項 7】

50

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項3または請求項4に記載のサーバ計算機保護装置。

【請求項8】

前記サーバ計算機の負荷状態を値として記憶する負荷状態記憶手段をさらに備え、
前記サーバ負荷算出手段は、求めた前記サーバ計算機の負荷状態に応じて前記負荷状態記憶手段に記憶した値を増減し、
前記データ要求転送手段は、前記負荷状態記憶手段に記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項3または請求項4に記載のサーバ計算機保護装置。

【請求項9】

一定期間内に、前記サーバ計算機から前記クライアント計算機への応答に含まれるパケット量を計測する応答量計測手段をさらに備え、
前記サーバ負荷検出手段は、前記応答量計測手段が計測したパケット量が多いほどより負荷が高いと算出することを特徴とする請求項5または請求項6に記載のサーバ計算機保護装置。

【請求項10】

前記サーバ計算機から前記クライアント計算機への応答があってから、該応答が再送されたことを検出する再応答検出手段をさらに備え、
前記サーバ負荷検出手段は、前記再応答検出手段が再送を検出すると、前記クライアント計算機のデータ要求による前記再送を行ったサーバ計算機の負荷がより高くなったと算出することを特徴とする請求項5または請求項6に記載のサーバ計算機保護装置。

【請求項11】

前記クライアント計算機との接続が強制的に切断され、または通信状態に異常があることを検出する通信状態検出手段をさらに備え、
前記サーバ負荷算出手段は、前記通信状態検出手段が通信異常を検出すると、前記クライアント計算機に対する前記サーバ計算機の負荷がより高くなったと算出することを特徴とする請求項5または請求項6に記載のサーバ計算機保護装置。

【請求項12】

前記クライアント計算機から新たな接続があったことを検出する接続検出手段をさらに備え、

前記サーバ負荷算出手段は、一定期間内に、前記接続検出手段が新たな接続を検出しない場合には、前記クライアント計算機に対する前記サーバ計算機の負荷がより低くなったと算出することを特徴とする請求項5または請求項6に記載のサーバ計算機保護装置。

【請求項13】

前記サーバ負荷算出手段は、前記処理情報受信手段が直前に受信した情報と、前記データ要求受け付け手段が受け付けたデータ要求の処理を前記サーバ計算機が開始した後の、該処理の実行中に受信した情報から、該サーバ計算機の負荷の差が所定の値よりも大きく上昇したと判断したときは前記クライアント計算機に対する前記サーバ計算機の負荷が高くなったと算出することを特徴とする請求項7または請求項8に記載のサーバ計算機保護装置。

【請求項14】

前記サーバ負荷算出手段は、前記処理情報受信手段が直前に受信した情報と、前記サーバ計算機が前記データ要求の処理を終了した直後に受信した情報から、前記直前に受信した情報と比べて、該サーバ計算機の負荷の差が所定の値よりも大きく低下したと判断したときは前記クライアント計算機に対する前記サーバ計算機の負荷が高いと算出することを特徴とする請求項7または請求項8に記載のサーバ計算機保護装置。

【請求項15】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項16】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項 17】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 15 または請求項 16 に記載のサーバ計算機保護方法。

【請求項 18】

前記データ要求転送ステップは、求めた前記サーバ計算機の前記クライアント計算機に対する負荷状態に応じて、予め記憶した値を増減し、
前記記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 15 または請求項 16 に記載のサーバ計算機保護方法。

【請求項 19】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護プログラム。

【請求項 20】

前記データ要求転送ステップは、求めた前記サーバ計算

機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 7 に記載のサーバ計算機保護プログラム。

【請求項 21】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、

所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、

所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、
一定期間内に、前記所定のクライアント計算機へ応答した数を計測するデータ供給数計測手段と、

前記データ要求数計測手段及びデータ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対する負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、
不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項 22】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、

所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、

所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、

前記サーバ計算機から、前記データ要求受け付け手段で受け付けた前記所定のクライアント計算機のデータ要求に対する、該サーバ計算機が実行している処理の状況に関する情報を受信する処理情報受信手段と

前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた

前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項 23】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とするサーバ計算機保護装置を備えた請求項 21 または請求項 22 に記載のサーバ計算機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、クライアントとなる計算機とサーバとなる計算機間のネットワークシステムに関し、特に、意図的にサーバ計算機の処理を妨害する不正なアクセスからサーバとなる計算機を保護するサーバ計算機保護装置に関する。

【0002】

【従来の技術】

近年、インターネット等を利用し、不特定あるいは特定のクライアントとなる計算機をネットワーク経由でサーバとなる計算機に接続し、クライアントからの要求に応じてサーバからデータを供給することを目的とするクライアント・サーバシステムが広く使われている。

【0003】

インターネット等のネットワークを流れるデータの形式として、宛先情報を付して伝送データを所定の大きさに再構成したパケットが一般に利用されている。パケットは、大まかに分けると、ヘッダとデータ本体とで構成されている。ヘッダには、このパケットの送り元である送信元の計算機を示す IP (Internet Protocol) アドレスと、このパケットの宛先となる計算機の IP アドレスといったアドレス情報をもっている。

【0004】

昨今、このようなネットワークに接続されたシステムに対し、システム的な障害を発生させることを目的としたネットワーク越しの攻撃が増加する傾向にある。たとえば、一つのクライアントから同時に大量のアクセス要求をサーバ計算機に対して行うことにより、攻撃対象となるサーバの稼働を妨げ実質的にサービスを不能にする攻

撃方法(以下、DoS攻撃(Denial of Service attack)と表記)がある。

【0005】

この攻撃方法は、システム攻撃を意図しない正当なクライアントからのアクセスとの区別が付きにくいために、サーバ側で攻撃を回避することが極めて困難である。場合によっては複数のクライアントからこの攻撃を受けることもあり、これを特にDDoS攻撃(Distributed Denial of Service attack)と呼んでいる。

10 【0006】

サーバへの要求がサーバの処理能力を超えるほど大量に送りつけられると、その要求毎に通信処理用の資源、たとえばメモリ領域や回線の帯域などが次々と確保されるためついには不足を来し、妨害を意図していない正当なクライアントからの要求に対しサーバが応答できなくなるか、あるいは大きく滞ってしまうという結果を招く。

【0007】

従来は、これらの攻撃を排除するためにサーバとネットワークの間にサーバ計算機保護装置を配置していた。このサーバ計算機保護装置は、複数回のアクセス要求が繰り返されたもののみを正当なアクセス要求として処理する、または既に正当なアクセスがあったクライアントからのアクセスを正当なアクセス要求として処理し、それ以外のアクセスについてはパケットを破棄するなどの処理を行っていた。

【0008】

しかし、このような方法では、攻撃を意図するクライアントが同じような大量のアクセス要求を行う場合、攻撃を排除できないという問題点があった。

【0009】

一方、上記問題を解決しても、たとえば特定のクライアントが大量のアクセス要求を行うとその通信行為がDoS攻撃であると判断されてしまうため、たとえそれが正当な要求であっても不正なアクセスとみなされる場合があった。DoS攻撃とみなされれば判断されたクライアントの接続は切断されてしまうため、そのクライアントで行っている業務に支障を来す。

【0010】

40 【特許文献1】 特開 2002-16633 公報

【0011】

【発明が解決しようとする課題】

本発明は、不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機を提供することを目的とする。

50 【0012】

【課題を解決するための手段】

本発明にかかるサーバ計算機保護装置とすれば、不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ供給数計測手段と、前記データ供給数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置が提供される。または、不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、前記サーバ計算機から該サーバ計算機の処理状況に関する情報を受信する処理情報受信手段と前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、を備えたことを特徴とするサーバ計算機保護装置が提供される。

【0013】

また本発明にかかるサーバ計算機保護方法によれば、不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、前記求めた負荷状態に応じて、一定期間内に受け付けた

前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、を有することを特徴とするサーバ計算機保護方法が提供される。

【0014】

加えて、本発明にかかるサーバ計算機保護プログラムとすれば、不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、を有することを特徴とするサーバ計算機保護プログラムが提供される。

【0015】

さらに、本発明にかかるサーバ計算機保護装置を備えたサーバ計算機が提供される。

【0016】

【発明の実施の形態】

(第1の実施形態)

図1に第1の実施形態におけるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図1では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント101-1、101-2、101-3と、ネットワーク102およびサーバ保護装置103が存在する。また、クライアント101で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置103を介して受信し、さらにサーバ計算機保護装置103を介して送信する計算機であるサーバ104とからなる。クライアント101はサーバ104へ処理に必要なデータを要求し、サーバ104はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント101とサーバ104との通信は、すべてサーバ計算機保護装置103を介して行われる。

【0017】

図2に第1の実施形態におけるサーバ計算機保護装置103の構成図の一例を示す。サーバ計算機保護装置103は、データ要求受け付け部201、データ要求転送部202、データ要求計測部203、データ供給数計測部204および応答確率算出部205からなる。

【0018】

クライアント101はサーバ計算機保護装置103を介してサーバ104との接続を確立した後、処理に必要なデータをサーバ104に対して要求する。このときデータ要求受け付け部201によって、サーバ104に対する要求を受け付けるとともに、データ要求数計測部203によって受け付け中の要求の数を計測する。

【0019】

データ要求受け付け部201によって受け付けられた要求は、データ要求転送部202によってサーバ104へと転送される。サーバ104はこの転送された要求に対するデータを、サーバ計算機保護装置103を介して、この要求を行ったクライアント101に向けて送信する。このときサーバ計算機保護装置103が備えるデータ供給数計測部204は、サーバ104のこの送信によって、受け付け済みの要求の完了数を計測する。つまりクライアント101に対してすべての応答が完了したときには、データ要求数計測部203で計測した受け付け中の要求数と、データ供給数計測部204で計測した完了済み要求数が一致することになる。

【0020】

仮に、データ要求数計測部203で計測された受け付け中の要求数が、データ供給数計測部204で計測した完了済み要求数よりも多い場合を考える。受け付け中の要求数が完了済み要求数よりも多いということはすなわち受け付けた要求に対する処理について、サーバ104の処理が遅れている（処理が重い）ことを意味する。完了済み要求数よりも受け付け中の要求数が増加していけば行くほどサーバ104の応答は遅延し、ひいてはサーバ104が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ104がクライアント101からDoS攻撃を受けた状態と同じである。サーバ104の管理者はサーバ104の停止を回避するため、クライアント101からサーバ104へ送信される要求を速やかに停止させなければならない。

【0021】

しかしながらクライアント101はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント101で稼動するアプリケーションの処理が中断あるいは処理そのものがないことになる。

【0022】

上記したような不具合を緩和するために、応答確率算出部205は受け付け中の要求数と完了済み要求数の差を元に、応答確率を少なくとも指示を行う都度算出し、こ

れをデータ要求転送部202に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント101からのデータ要求の数に対して、サーバ104が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部202は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ104へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ104へ転送するデータ要求の数を減らす。

【0023】

一定期間内に転送される要求数を減らしたために、データ要求転送部202によって転送されなかったデータ要求は、データ要求受け付け部201から破棄される。あるいは破棄することなくデータ要求受け付け部201に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【0024】

応答確率算出部205は、受け付け中の要求数と完了済み要求数との差が少なくなるとサーバ104の負荷が軽いと判断して応答確率を高く算出し、また各要求数の差が大きくなるとサーバ104の負荷が高いと判断し応答確率を低く算出する。

【0025】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【0026】

なお、データ要求数計測部203の受け付け中の要求数とデータ供給数計測部204が計測する完了済み要求数のそれぞれの数は、たとえば前者を加算、後者を減算するようにして差分値のみを保持するようにしてもよい。結果的に両者の比較が可能な手段で蓄積されていれば足りる。

【0027】

図3に第1の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【0028】

サーバ計算機保護装置103を介してクライアント101からサーバ104への接続が確立された後、クライアント101からサーバ104に向けてデータ要求がされるのを待つ（S1）。データの要求がされたならばデータ要求数計測部203によって、応答確率算出部205が保持する受け付け中の要求数を1増加させる（S2）。

【0029】

データ要求受け付け部201によって受け付けられたク

クライアント101からのデータ要求は、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断される(S3)。ステップS3の判断に際しては、未完了の受け付け中の要求数が使用される。一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほどサーバ104の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ104がデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0030】

上記したような理由からステップS3の判定に、未完了の受け付け要求数を、サーバ104の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ104がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップS3では、この未完了の受け付け要求数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆に多ければDoS攻撃を受けている可能性があるため新たなデータ要求を破棄すべきと判断する。

【0031】

さらに以下に説明する基準も、応答確率算出部205が算出し、データ要求転送部202が転送するデータ要求の応答確率に反映することができる。

【0032】

通信データにはデータ量を示す情報が付加されているため、データ供給数計測部204でサーバ104がクライアント101からのデータ要求に対するデータ応答のデータ量を計測することができる。応答するデータ量が多いということはサーバ104が応答データを作成するのに多くのコストを費やしていることを意味している。加えてこの通信に費やす時間も多くなり、通信回線の占有時間が長くなる。サーバ104の処理負荷及び通信回線の占有もまた、サーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0033】

図3に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、このデータ応答のデータ量が考慮される。

【0034】

ステップS3では、このデータ応答のデータ量に応じて

クライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。データ量がより少なければサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆に多ければDoS攻撃を受けている可能性があるため新たなデータ要求を破棄すべきと判断する。

【0035】

データ要求と、サーバ104が対応するデータ応答とはそれぞれ対応した順番号が付与されている。このためあるデータ応答がどのデータ要求のものが特定することができる。

【0036】

このとき、クライアント101からのあるデータ要求に対しサーバ104が応答したとする。その後、クライアント101からこのデータ応答に対する確認応答が所定時間得られなかったとすると、サーバ104は先のデータ応答がクライアント101に到達しなかったと判断して再送を試みる。データ供給数計測部204は、上述したように、再送したデータ応答はどのデータ要求の応答であるかが特定することができる。

【0037】

この仕組みはサーバ104がクライアント101に対して確実に通信を行うための手段であるが、クライアント101が意図的に確認応答を返さない場合も考えられる。するとサーバ104は際限なく再送を繰り返し、ひいては無用な処理負荷を伴い、同時に無用な再送により通信回線も占有してしまう。この場合もまたサーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0038】

図3に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、このデータ応答の再送回数が考慮される。

【0039】

ステップS3では、このデータ応答の再送回数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。再送回数が多ければ多いほどDoS攻撃を受けている可能性があるため新たなデータ要求を破棄すべきと判断する。

【0040】

データ要求受け付け部201は、サーバ104の代理としてクライアント101からのデータ要求を受け付ける。このとき、クライアント101が要求し、サーバ104と接続したコネクションが不当に切断されると、データ要求受け付け部201はこの不当な切断を検出することができる。不当な切断とは、例えば通信に使用するプロトコルに適合しない異常なコマンドの送出またはフローなどにより、正常な通信が維持できなくなったことを検出し切断されてしまうことをいう。またクライアン

ト101からの一方的な強制切断要求などを受けることも含まれる。

【0041】

サーバ104は、異常なコマンドやフローまたは強制切断要求を受け取るとこれらは予期しないデータであることから通信資源のリカバリ処理を行わねばならなくなる。サーバ104内で稼動する更新アプリケーションがあった場合には、上記リカバリ処理の中でロールバックなどの更新取り消し処理が必要となることも考えられる。これらの処理はサーバ104に対し多大な負荷を与えることが多い。このような異常な通信が繰り返し行われるとサーバ104の負荷が上がり、サーバ104全体の処理効率が著しく低下する。この場合もまたサーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0042】

図3に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、この異常な通信の回数が考慮される。

【0043】

ステップS3では、この異常な通信の回数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0044】

上記のように、いくつかの判断基準を設けることにより効果的にDoS攻撃を防止することが可能となる。

【0045】

応答確率算出部205の応答確率の算出に際して、この応答確率算出部205の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【0046】

データ要求数計測部203、データ供給数計測部204及びデータ要求受け付け部201から取得した情報を基に応答確率算出部205はサーバ104の負荷を判断する。このとき、算出した値をそのままサーバ104の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【0047】

例えば、各計測部から得られた値を総合して0から10までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては0から10まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【0048】

そこで、各計測部から得られた値を総合して±2の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±2の範囲でしか変動しないため、応答確率記憶部が0から10までの値を保持するものとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【0049】

仮に応答確率の変動があまりに急に行われるとサーバ104にかかる負荷が一定せず、サーバ104が不安定になる場合がある。

【0050】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント101からサーバ104に到達するデータ要求数の変動を緩和し、サーバ104を保護することができる。

【0051】

このときサーバ104にクライアント101からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ104に転送する(S4)。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部201から破棄し、再びクライアント101からの新たなデータ要求を待つ(S1)。

【0052】

クライアント101からのデータ要求をサーバ104に転送したときには、次にこのデータ要求に対するサーバ104からの応答があるので、これをクライアント101に対して転送する(S5)。

【0053】

そしてこの応答からデータ供給数計測部204によって完了済みの要求を計測し、応答確率算出部205が保持する受け付け中の要求数を1減少させる(S6)。クライアント101からサーバ104への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント101からサーバ104に向けて新たなデータ要求がされるのを待つ(S1)。

【0054】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【0055】

(第2の実施形態)

図1に第2の実施形態における、サーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図1では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント101-1、101-2、101

ー 3 と、ネットワーク 102 およびサーバ保護装置 103 が存在する。また、クライアント 101 で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置 103 を介して受信し、さらにサーバ計算機保護装置 103 を介して送信する計算機であるサーバ 104 とからなる。クライアント 101 はサーバ 104 へ処理に必要なデータを要求し、サーバ 104 はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント 101 とサーバ 104 との通信は、すべてサーバ計算機保護装置 103 を介して行われる。

【0056】

図 4 に第 2 の実施形態におけるサーバ計算機保護装置 103 の構成図の一例を示す。サーバ計算機保護装置 103 は、データ要求受け付け部 201、データ要求転送部 202、データ要求計測部 203、データ供給数計測部 204 および応答確率算出部 205 からなる。図 2 に示した第 1 の実施形態におけるサーバ計算機保護装置 103 との相違は、データ要求数計測部 203 及び応答確率算出部 205 を複数備えていることである。これら複数の各計測部は、複数あるクライアント 101（たとえばクライアント 101-1、101-2、101-3）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示す IP アドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示す IP アドレスを参照することにより判別可能である。

【0057】

各構成要素の動作は第 1 の実施形態のものと同じである。

【0058】

図 5 に第 2 の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【0059】

サーバ計算機保護装置 103 を介してクライアント 101 からサーバ 104 への接続が確立され、そのクライアント 101 にデータ要求数計測部 203 と応答確率算出部 205 の組が割り当てられた後、クライアント 101 からサーバ 104 に向けてデータ要求がされるのを待つ（S1）。データの要求がされたならばそのデータ要求を行ったクライアント 101 に割り当てられているデータ要求数計測部 203 によって、その組となっている応答確率算出部 205 が保持する受け付け中の要求数を 1 増加させる（S7）。

【0060】

データ要求受け付け部 201 によって受け付けられた所定のクライアント 101 からのデータ要求は、データ要求転送部 202 によってサーバ 104 へ転送しても良いものかどうか判断される（S3）。ステップ S3 の判断に際しては、未完了の受け付け中の要求数が使用される。

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほど所定のクライアント 101 によるサーバ 104 の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ 104 が所定のクライアント 101 によるデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ 104 は DoS 攻撃を受けている可能性が高いと判断できる。

【0061】

上記したような理由からステップ S3 の判定に、未完了の受け付け要求数を、サーバ 104 の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ 104 が DoS 攻撃を受けていかどうかという判別にも使用できることを意味している。ステップ S3 では、この未完了の受け付け要求数に応じて所定のクライアント 101 からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ 104 に余裕があるので新たなデータ要求を転送すべきと判断し、逆に多ければ DoS 攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0062】

さらに以下に説明する基準も、応答確率算出部 205 が算出し、データ要求転送部 202 が転送するデータ要求の応答確率に反映することができる。

【0063】

通信データにはデータ量を示す情報が付加されているため、データ供給数計測部 204 でサーバ 104 がクライアント 101 からのデータ要求に対するデータ応答のデータ量を計測することができる。応答するデータ量が多いということはサーバ 104 が応答データを作成するのに多くのコストを費やしていることを意味している。加えてこの通信に費やす時間も多くなり、通信回線の占有時間が長くなる。サーバ 104 の処理負荷及び通信回線の占有もまた、サーバ 104 は DoS 攻撃を受けている可能性が高いと判断できる。

【0064】

図 3 に示した、データ要求受け付け部 201 によって受け付けられたクライアント 101 からのデータ要求が、データ要求転送部 202 によってサーバ 104 へ転送し

ても良いものかどうか判断されるステップS3の判断に際しては、このデータ応答のデータ量が考慮される。

【0065】

ステップS3では、このデータ応答のデータ量に応じてクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。データ量がより少なければサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆に多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0066】

データ要求と、サーバ104が対応するデータ応答とはそれぞれ対応した順番号が付与されている。このためあるデータ応答がどのデータ要求のものが特定することができる。

【0067】

このとき、クライアント101からのあるデータ要求に対しサーバ104が応答したとする。その後、クライアント101からこのデータ応答に対する確認応答が所定時間得られなかったとすると、サーバ104は先のデータ応答がクライアント101に到達しなかったと判断して再送を試みる。データ供給数計測部204は、上述したように、再送したデータ応答はどのデータ要求の応答であるかが特定することができる。

【0068】

この仕組みはサーバ104がクライアント101に対して確実に通信を行うための手段であるが、クライアント101が意図的に確認応答を返さない場合も考えられる。するとサーバ104は際限なく再送を繰り返し、ひいては無用な処理負荷を伴い、同時に無用な再送により通信回線も占有してしまう。この場合もまたサーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0069】

図3に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、このデータ応答の再送回数が考慮される。

【0070】

ステップS3では、このデータ応答の再送回数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。再送回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0071】

データ要求受け付け部201は、サーバ104の代理としてクライアント101からのデータ要求を受け付ける。このとき、クライアント101が要求し、サーバ104と接続したコネクションが不当に切断されると、データ要求受け付け部201はこの不当な切断を検出する

ことができる。不当な切断とは、例えば通信に使用するプロトコルに適合しない異常なコマンドの送出またはフローなどにより、正常な通信が維持できなくなったことを検出し切断されてしまうことをいう。またクライアント101からの一方的な強制切断要求などを受けることも含まれる。

【0072】

サーバ104は、異常なコマンドやフローまたは強制切断要求を受け取るとこれらは予期しないデータであることから通信資源のリカバリ処理を行わねばならなくなる。サーバ104内で稼動する更新アプリケーションがあった場合には、上記リカバリ処理の中でロールバックなどの更新取り消し処理が必要となることも考えられる。これらの処理はサーバ104に対し多大な負荷を与えることが多い。このような異常な通信が繰り返し行われるとサーバ104の負荷が上がり、サーバ104全体の処理効率が著しく低下する。この場合もまたサーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0073】

図3に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、この異常な通信の回数が考慮される。

【0074】

ステップS3では、この異常な通信の回数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0075】

上記のように、いくつかの判断基準を設けることにより効果的にDoS攻撃を防止することが可能となる。

【0076】

応答確率算出部205の応答確率の算出に際して、この応答確率算出部205の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【0077】

データ要求数計測部203、データ供給数計測部204及びデータ要求受け付け部201から取得した情報を基に、応答確率算出部205は各クライアントが掛けているサーバ104の負荷を判断する。このとき、算出した値をそのままサーバ104の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【0078】

例えば、各計測部から得られた値を総合して0から10までの負荷レベルを示す値に変換していたものとする。

各計測部から得られる値によっては0から10まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【0079】

そこで、各計測部から得られた値を総合して±2の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±2の範囲でしか変動しないため、応答確率記憶部が0から10までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【0080】

仮に応答確率の変動があまりに急に行われるとサーバ104にかかる負荷が一定せず、サーバ104が不安定になる場合がある。

【0081】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント101からサーバ104に到達するデータ要求数の変動を緩和し、サーバ104を保護することができる。

【0082】

このときサーバ104に所定のクライアント101からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ104に転送する(S8)。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部201から破棄し、再び所定のクライアント101からの新たなデータ要求を待つ(S1)。

【0083】

所定のクライアント101からのデータ要求をサーバ104に転送したときには、次にこのデータ要求に対するサーバ104からの応答があるので、これを所定のクライアント101に対して転送する(S5)。

【0084】

そしてこの応答からデータ供給数計測部204によって完了済みの要求を計測し、所定のクライアント101に割り当てられた応答確率算出部205が保持する受け付け中の要求数を1減少させる(S9)。所定のクライアント101からサーバ104への接続が確立されたままならば再び同様の動作フローを繰り返し、所定のクライアント101からサーバ104に向けて新たなデータ要求がされるのを待つ(S1)。

【0085】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【0086】

(第3の実施形態)

図1に第3の実施形態におけるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図1では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント101-1、101-2、101-3と、ネットワーク102およびサーバ保護装置103が存在する。また、クライアント101で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置103を介して受信し、さらにサーバ計算機保護装置103を介して送信する計算機であるサーバ104とからなる。クライアント101はサーバ104へ処理に必要なデータを要求し、サーバ104はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント101とサーバ104との通信は、すべてサーバ計算機保護装置103を介して行われる。

【0087】

図6に第3の実施形態におけるサーバ計算機保護装置103の構成図の一例を示す。サーバ計算機保護装置103は、データ要求受け付け部201、データ要求転送部202、応答確率算出部205および処理状況受信部206からなる。

【0088】

クライアント101はサーバ計算機保護装置103を介してサーバ104との接続を確立した後、処理に必要なデータをサーバ104に対して要求する。このときデータ要求受け付け部201によって、サーバ104に対する要求を受け付ける。

【0089】

データ要求受け付け部201によって受け付けられた要求は、データ要求転送部202によってサーバ104へと転送される。サーバ104はこの転送された要求に対するデータを、サーバ計算機保護装置103を介して、この要求を行ったクライアント101に向けて送信する。

【0090】

処理状況受信部206はサーバ104から、サーバ104自身の処理状況についての情報を受信する。具体的には、たとえばサーバ104の送信時の負荷状況などである。サーバ104が通知する情報にはデータ要求受け付け部201が受け付けたデータ要求と、サーバ104が処理している状況あるいは処理した結果とが結び付けられて格納されていても良い。この場合はたとえば、あるデータ要求と、このデータ要求を処理するために起動したアプリケーションがサーバ104に対して掛けた負荷とが関連することが分かるような情報である。

【0091】

所定の時間間隔あるいは任意のタイミングで所得した、サーバ104から得られた処理状況情報を分析すると、

クライアント101が要求したデータ要求とサーバ104の負荷状況との関係が分かる。たとえば、クライアント101からあるデータ要求があった後にサーバ104の負荷が急激に変動するような特徴が発見できる。もしもサーバ104の負荷を急激に上げるようなデータ要求を立て続けに行うクライアント101があった場合には、サーバ104の処理能力を著しく消費する。ひいてはサーバ104が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ104がクライアント101からDoS攻撃を受けた状態と同じである。サーバ104の管理者はサーバ104の停止を回避するため、クライアント101からサーバ104へ送信される要求を速やかに停止させなければならない。

【0092】

しかしながらクライアント101はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント101で稼動するアプリケーションの処理が中断あるいは処理そのものができないことになる。

【0093】

上記したような不具合を緩和するために、応答確率算出部205は処理状況情報を元に、応答確率を少なくともサーバ104から情報を取得する都度算出し、これをデータ要求転送部202に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント101からのデータ要求の数に対して、サーバ104が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部202は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ104へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ104へ転送するデータ要求の数を減らす。

【0094】

一定期間内に転送される要求数を減らしたために、データ要求転送部202によって転送されなかったデータ要求は、データ要求受け付け部201から破棄される。あるいは破棄することなくデータ要求受け付け部201に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【0095】

応答確率算出部205は、サーバ104から所得した処理状況情報からサーバ104の負荷が軽いと判断すると応答確率を高く算出し、またサーバ104の負荷が高いと判断すれば応答確率を低く算出する。

【0096】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させるこ

とのないサーバ計算機保護装置とすることができる。

【0097】

図7に第3の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【0098】

図7 (A) に示すフローは、サーバ104から処理状況情報を取得するためのものである。一方、図7 (B) はクライアント101からデータ要求を受け付け、サーバ104に受け渡すフローを示している。これら二つのフローはそれぞれ非同期に処理される。

【0099】

まず図7 (A) について説明する。処理状況受信部206は、サーバ104から、このサーバが行っている処理の状況についての情報を取得すべく、この情報が送信されるのを待つ (S10)。情報が正常に所得できたかどうかを判断し (S11)、正常に取得できた場合には処理状況受信部206はこのサーバ104についての処理負荷を確定する (S12)。この処理はサーバ104から処理状況情報を取得する都度実行し、サーバ104の処理負荷の状況をリアルタイムに確定する。

【0100】

ステップS11にて処理状況情報が取得できなかった場合は、再びこの情報が送信されるのを待つ (S10)。

【0101】

次に図7 (B) について説明する。

【0102】

サーバ計算機保護装置103を介してクライアント101からサーバ104への接続が確立された後、クライアント101からサーバ104に向けてデータ要求がされるのを待つ (S1)。

【0103】

データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求は、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断される (S3)。ステップS3の判断に際しては、処理状況受信部206が確定したサーバ104についての処理負荷が使用される。

負荷が低ければサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆により高ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0104】

さらに以下に説明する基準も、応答確率算出部205が算出し、データ要求転送部202が転送するデータ要求の応答確率に反映することができる。

【0105】

サーバ104の処理状況情報を取りつづけていると、データ要求とサーバ104の負荷に特徴を見つけることができる場合がある。たとえば、データ要求受け付け部201が受け付け、データ要求転送部202がデータ要求

を転送した後に、決まってサーバ104の処理が急激に上昇するような場合である。

このような処理負荷が急激に上がるような傾向が見つかり、サーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0106】

図7に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、この処理負荷が急激に上がる傾向があるかどうか考慮される。

【0107】

ステップS3では、負荷のかかり方の傾向を判断しクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。負荷が急激に上がる傾向があるならばDoS攻撃を受けている可能性があるため新たなデータ要求を破棄すべきと判断する。

【0108】

逆に、クライアント101からのデータ要求が無くなったとたん、サーバ104の負荷が急激に低下する場合もある。このような処理負荷が急激に下がるような傾向が見つかり、サーバ104はDoS攻撃を受けていた可能性が高いと判断できる。

【0109】

図7に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断されるステップS3の判断に際しては、この処理負荷が急激に下がる傾向があるかどうか考慮される。

【0110】

ステップS3では、負荷のかかり方の傾向を判断しクライアント101からの新たなデータ要求を転送しても良いかどうか判断材料とする。負荷が急激に下がる傾向があるならばDoS攻撃を受けていた可能性があるため新たなデータ要求は安易に受け付けず破棄すべきと判断する。

【0111】

応答確率算出部205の応答確率の算出に際して、この応答確率算出部205の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【0112】

処理状況受信部206が受信した、サーバ104の処理状況情報を基に応答確率算出部205はサーバ104の負荷を判断する。このとき、算出した値をそのままサーバ104の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【0113】

例えば、各計測部から得られた値を総合して0から10までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては0から10まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【0114】

そこで、各計測部から得られた値を総合して±2の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±2の範囲でしか変動しないため、応答確率記憶部が0から10までの値を保持するものだとなれば、先の例のように応答確率が大きく変動することを抑制することができる。

【0115】

仮に応答確率の変動があまりに急に行われるとサーバ104にかかる負荷が一定せず、サーバ104が不安定になる場合がある。

【0116】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント101からサーバ104に到達するデータ要求数の変動を緩和し、サーバ104を保護することができる。

【0117】

このときサーバ104にクライアント101からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ104に転送する(S4)。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部201から破棄し、再びクライアント101からの新たなデータ要求を待つ(S1)。

【0118】

クライアント101からのデータ要求をサーバ104に転送したときには、次にこのデータ要求に対するサーバ104からの応答があるので、これをクライアント101に対して転送する(S5)。クライアント101からサーバ104への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント101からサーバ104に向けて新たなデータ要求がされるのを待つ(S1)。

【0119】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【0120】

(第4の実施形態)

図1に第4の実施形態における、サーバ計算機保護装置

が適用されるネットワーク構成図の一例を示す。図1では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント101-1、101-2、101-3と、ネットワーク102およびサーバ保護装置103が存在する。また、クライアント101で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置103を介して受信し、さらにサーバ計算機保護装置103を介して送信する計算機であるサーバ104とからなる。クライアント101はサーバ104へ処理に必要なデータを要求し、サーバ104はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント101とサーバ104との通信は、すべてサーバ計算機保護装置103を介して行われる。

【0121】

図8に第4の実施形態におけるサーバ計算機保護装置103の構成図の一例を示す。サーバ計算機保護装置103は、データ要求受け付け部201、データ要求転送部202、応答確率算出部205及び処理状況受信部206からなる。図6に示した第3の実施形態におけるサーバ計算機保護装置103との相違は、応答確率算出部205を複数備えていることである。これら複数の各計測部は、複数あるクライアント101（たとえばクライアント101-1、101-2、101-3）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示すIPアドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示すIPアドレスを参照することにより判別可能である。

【0122】

各構成要素の動作は第3の実施形態のものと同じである。

【0123】

図9に第4の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【0124】

図9(A)に示すフローは、サーバ104から処理状況情報を取得するためのものである。一方、図9(B)はクライアント101からデータ要求を受け付け、サーバ104に受け渡すフローを示している。これら二つのフローはそれぞれ非同期に処理される。

【0125】

まず図9(A)について説明する。処理状況受信部206は、サーバ104から、このサーバが行っている処理の状況についての情報を取得すべく、この情報が送信さ

れるのを待つ(S10)。情報が正常に所得できたかどうかを判断し(S11)、正常に取得できた場合には処理状況受信部206はこのサーバ104に各クライアントが掛けている処理負荷をクライアントごとに確定する(S13)。この処理はサーバ104から処理状況情報を取得する都度実行し、各クライアントが掛けているサーバ104の処理負荷の状況をリアルタイムに確定する。

【0126】

ステップS11にて処理状況情報が取得できなかった場合は、再びこの情報が送信されるのを待つ(S10)。

【0127】

次に図7(B)について説明する。

【0128】

サーバ計算機保護装置103を介してクライアント101からサーバ104への接続が確立され、そのクライアント101に応答確率算出部205が割り当てられた後、クライアント101からサーバ104に向けてデータ要求がされるのを待つ(S1)。

【0129】

データ要求受け付け部201によって受け付けられた所定のクライアント101からのデータ要求は、データ要求転送部202によってサーバ104へ転送しても良いものかどうか判断される(S3)。ステップS3の判断に際しては、処理状況受信部206が確定したサーバ104についての処理負荷が使用される。負荷が低ければ所定のクライアントについてサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆に高ければそのクライアントからDoS攻撃を受けている可能性があるため新たなデータ要求を破棄すべきと判断する。

【0130】

さらに以下に説明する基準も、応答確率算出部205が算出し、データ要求転送部202が転送するデータ要求の応答確率に反映することができる。

【0131】

サーバ104の処理状況情報を取りつづけていると、各クライアントからのデータ要求とサーバ104の負荷に特徴を見つけることができる場合がある。たとえば、データ要求受け付け部201が受け付け、データ要求転送部202がデータ要求を転送した後に、決まってサーバ104の処理が急激に上昇するような場合である。所定のクライアントについて、このような処理負荷が急激に上がるような傾向が見つかると、サーバ104はこのクライアントからDoS攻撃を受けている可能性が高いと判断できる。

【0132】

図9に示した、データ要求受け付け部201によって受け付けられたクライアント101からのデータ要求が、データ要求転送部202によってサーバ104へ転送し

ても良いものかどうか判断されるステップ S 3 の判断に際しては、この処理負荷が急激に上がる傾向があるかどうか考慮される。

【0133】

ステップ S 3 では、負荷のかかり方の傾向を判断しクライアント 101 からの新たなデータ要求を転送しても良いかどうか判断材料とする。所定のクライアントについて負荷が急激に上がる傾向があるならばそのクライアントから DoS 攻撃を受けている可能性があるため、そのクライアントからの新たなデータ要求を破棄すべきと判断する。

【0134】

逆に、クライアント 101 からのデータ要求が無くなったとたん、サーバ 104 の負荷が急激に低下する場合もある。所定のクライアントについて、このような処理負荷が急激に下がるような傾向が見つかると、サーバ 104 はそのクライアントから DoS 攻撃を受けていた可能性が高いと判断できる。

【0135】

図 9 に示した、データ要求受け付け部 201 によって受け付けられたクライアント 101 からのデータ要求が、データ要求転送部 202 によってサーバ 104 へ転送しても良いものかどうか判断されるステップ S 3 の判断に際しては、この処理負荷が急激に下がる傾向があるかどうか考慮される。

【0136】

ステップ S 3 では、負荷のかかり方の傾向を判断しクライアント 101 からの新たなデータ要求を転送しても良いかどうか判断材料とする。負荷が急激に下がる傾向があるならばそのクライアントから DoS 攻撃を受けていた可能性があるため、そのクライアントからの新たなデータ要求は安易に受け付けず破棄すべきと判断する。

【0137】

応答確率算出部 205 の応答確率の算出に際して、この応答確率算出部 205 の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【0138】

処理状況受信部 206 が受信した、サーバ 104 の処理状況情報を基に応答確率算出部 205 は各クライアントが掛けているサーバ 104 の負荷を判断する。このとき、算出した値をそのままサーバ 104 の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【0139】

例えば、各計測部から得られた値を総合して 0 から 10 までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては 0 から 10 まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【0140】

そこで、各計測部から得られた値を総合して ± 2 の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で ± 2 の範囲でしか変動しないため、応答確率記憶部が 0 から 10 までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【0141】

仮に応答確率の変動があまりに急に行われるとサーバ 104 にかかる負荷が一定せず、サーバ 104 が不安定になる場合がある。

【0142】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント 101 からサーバ 104 に到達するデータ要求数の変動を緩和し、サーバ 104 を保護することができる。

【0143】

このときサーバ 104 に所定のクライアント 101 からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ 104 に転送する (S 8)。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部 201 から破棄し、再び所定のクライアント 101 からの新たなデータ要求を待つ (S 1)。

【0144】

所定のクライアント 101 からのデータ要求をサーバ 104 に転送したときには、次にこのデータ要求に対するサーバ 104 からの応答があるので、これを所定のクライアント 101 に対して転送する (S 5)。

【0145】

所定のクライアント 101 からサーバ 104 への接続が確立されたままならば再び同様の動作フローを繰り返し、所定のクライアント 101 からサーバ 104 に向けて新たなデータ要求がされるのを待つ (S 1)。

【0146】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるような DoS 攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらず DoS 攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【0147】

(各実施形態における変形例)

各実施形態の変形例として、サーバ 104 に本実施形態にかかるサーバ計算機保護装置 103 の構成を組み込んだサーバ 104 とすることができる。このように構成するとクライアント 101 からのデータ要求を処理するサーバ 104 と、このサーバ 104 を不特定のクライアン

ト 101 からのDoS攻撃から保護する目的で設けるサーバ計算機保護装置 103 とを分離して個別に構築する必要がない。よってサーバ計算機保護装置 103 とサーバ 104 との通信をネットワーク等を介して行う必要もなくなり、代理応答の通信に要していた時間を排除することができる。また複数の筐体により構成したサーバ計算機保護装置 103 によって保護されたサーバ 104 の場合と比較して、同様の機能を 1 つの筐体で提供できる可能性があり、この場合には設置に必要なスペースを削減することができる。

【0148】

【発明の効果】

不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置とすることができる。

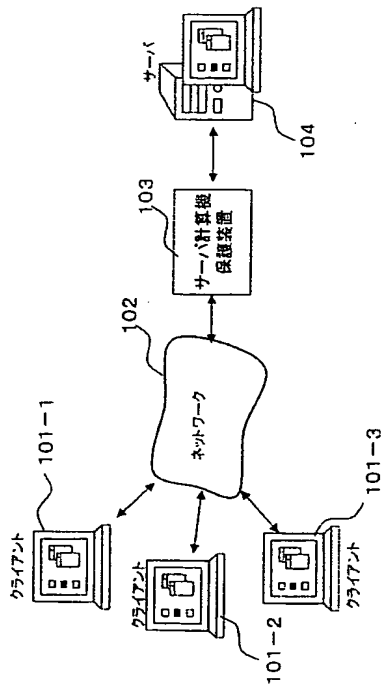
【図面の簡単な説明】

【図 1】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す図である。

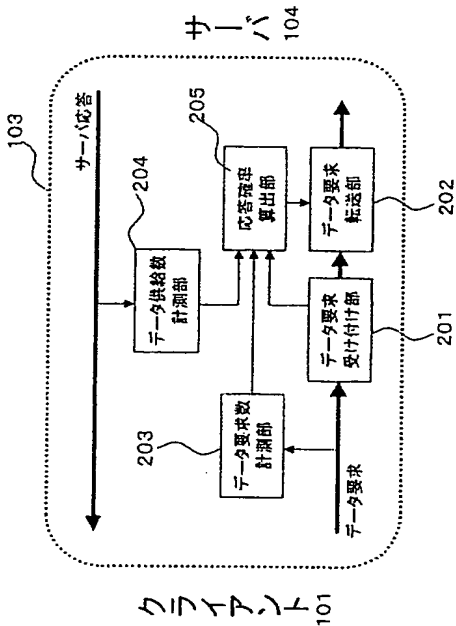
【図 2】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 3】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

【図 1】



【図 2】



【図 4】 本発明の第 2 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 5】 本発明の第 2 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

【図 6】 本発明の第 3 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 7】 本発明の第 3 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

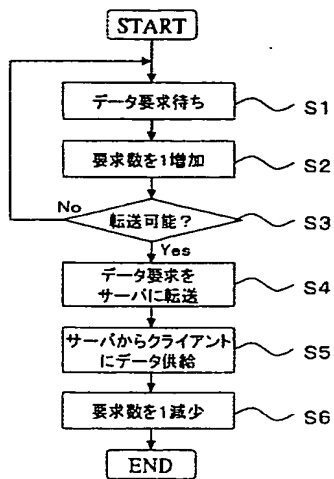
【図 8】 本発明の第 4 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 9】 本発明の第 4 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

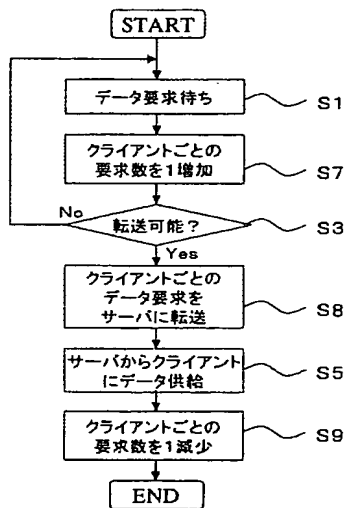
【符号の説明】

- 101-1 . . . クライアント
- 101-2 . . . クライアント
- 101-3 . . . クライアント
- 102 . . . ネットワーク
- 103 . . . サーバ計算機保護装置
- 104 . . . サーバ
- 201 . . . データ要求受け付け部
- 202 . . . データ要求転送部
- 203 . . . データ要求数計測部
- 204 . . . データ供給数計測部
- 205 . . . 応答確率算出部
- 206 . . . 処理状況受信部

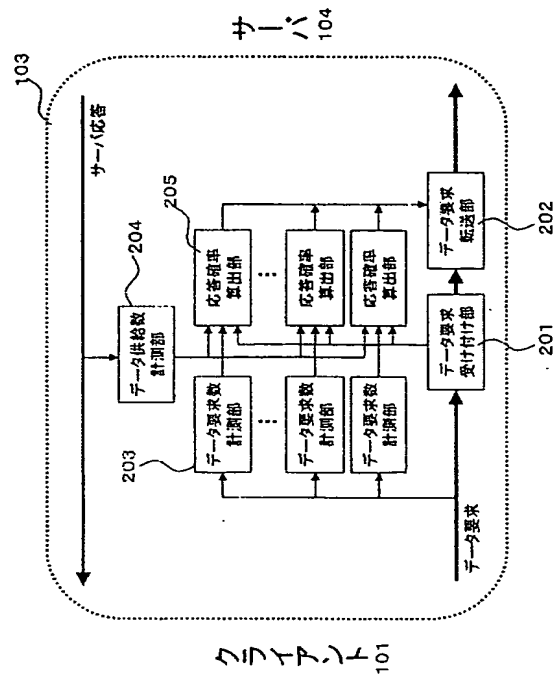
【図3】



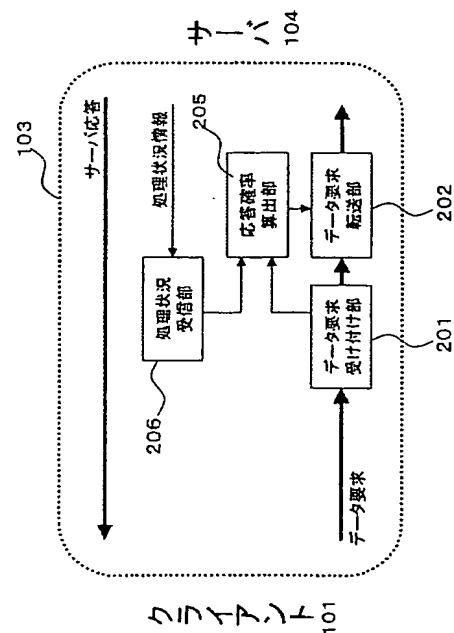
【図5】



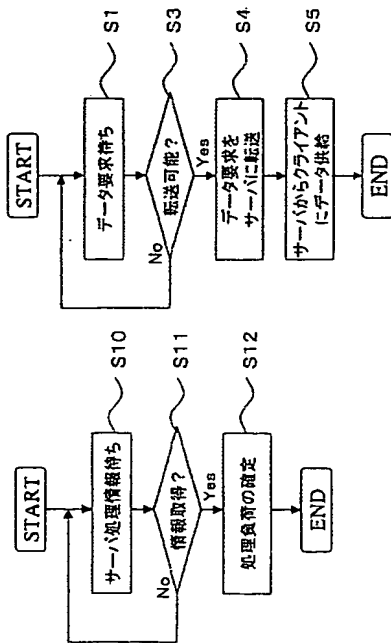
【図4】



【図6】



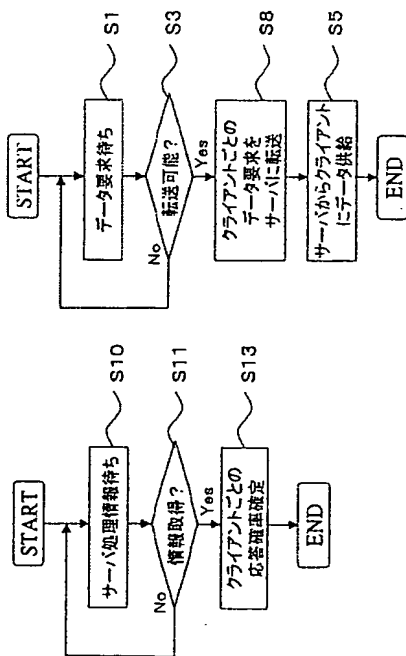
【図7】



(B)

(A)

【図9】



(B)

(A)

【図8】

